Simple Safety Checks:

Make sure your account and devices are safe.

Your personal information is constantly being targeted. Identity theft, phishing attempts, spoofed emails, company breaches, or scams – this multi-billion dollar industry is always growing and evolving. If the most recent fraud attempt has you wondering how you can protect yourself moving forward, you aren't alone. Just as you do regular maintenance on your car and home, or go to the doctor for a check-up, you need to schedule time for maintenance for your accounts and devices in order to help keep you safe, secure, and protected.

Here are the seven things you should do regularly to keep your accounts and devices safe.

1. **Check and change your passwords**

You know you're not supposed to use the same password for multiple accounts, but you still do it. You are not alone. An incredible **92% of people admit they use the same password for many accounts for multiple sites.** Fraudsters know this too.

Remember these tips when it comes to passwords:

- Use unique passwords in different systems and accounts
- **Mix it up.** Use a combination of capital and lowercase letters, numbers, and special characters and are at least eight characters long
- Try to choose your own security questions when possible. Standard security questions don't cut it anymore. Passwords that are based on personal information might easily be guessed by simply checking out your social media

- Develop mnemonics such as passphrases and acronyms for remembering complex passwords
- **Don't leave your passwords on sticky notes** attached to your monitor or under your keyboard. You don't leave your house key under your mat anymore (hopefully) because the bad guys look there first. It's the same philosophy here. If you must write them down, keep them hidden, preferably locked away somewhere separate from your computer or mobile device.

2. Check your activity and check it often

This isn't just about looking at your financial transactions, but all of your online logins. The specifics vary from service to service, but you can view your most recent logins and devices where your account has been authorized. This is important in being able to find (and block) any devices you don't recognize.

In some apps and services, you can **enable alerts (typically via text or email)** that get activated whenever you or someone else logs in on a new device.

Cheney Federal Credit Union provides tools like our mobile app, online banking, and text banking to view new transactions and charges. CFCU's VISA debit and credit cards are monitored for fraudulent activity and might reach out to you if fraud is suspected.

Creating alerts to notify you about important transactions is just one of the services CFCU offers.

3. Check your connected apps

You know that pop-up that magically appears when you log into your account online? The one that conveniently asks if you want it to 'remember' your password? It may be super handy but just consider if that awesome password manager were to be hacked.

Third-party apps and add-ons are inherently dangerous and you're fine to keep using them, just proceed with caution.

4. Check what's running on your computer

Task Manager (search for it in the taskbar on Windows) and Activity Monitor (search for it in Spotlight on macOS) will give you a list of everything in memory on your system – run a quick web search on anything you don't understand and do the same for any browser plug-ins and add-ons you either don't remember installing or no longer have any need for. This will probably help speed up your computer from being bogged down with apps as well.

5. **Check the permissions of your installed apps**

There has been a lot of conversation around this. **Apps do more than just provide you that fun game - they can also be capturing your location, behaviors, and more.** Recent versions of both Android and iOS now let you manage permissions one-by-one for your apps. On Android open settings, then tap Apps & Notifications, App info, and then the app of your choice to see the permissions. On iOS, choose an app from the main list is Settings, or select Privacy from Settings to see the permissions grouped by their type.

6. **Check what you send over public Wi-Fi**

Remember 3-Way phone calls? You could call a friend and then bring in another friend on the call for a "party line". It was an early way to conference call. The problem was if you were the last person to join the call, you didn't necessarily know everyone on the call. Public Wi-Fi is very similar. Being on the same network makes it a whole lot easier for fraudsters to listen in. This is also one of the reasons you should be leery of using Wi-Fi at public places like hotels and coffee shops. **Be cautious if using public Wi-Fi for anything sensitive.**

7. **Check for updates**

Update, update, update – getting the latest patches and upgrades installed is so important to the security of your devices that it's now very difficult to avoid applying them on Windows, macOS, Android, and iOS. It's still worth mentioning though, and still worth checking both for the operating systems you're using and the apps running on top.

If you feel you have been a victim of identity theft or fraud, contact Cheney Federal Credit Union at **509.235.6533**